# RFC 2350 CSIRT MIKA (MITRA KELUARGA)

## 1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi CSIRT MIKA berdasarkan RFC 2350, yaitu informasi dasar mengenai CISRT MIKA, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CSIRT MIKA

### 1.1. Tanggal Update Terakhir

Dokumen merupkan dokumen versi 1.0 yang diterbitkan pada tanggal dd month yyyy.

### 1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

### 1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

https://csirt.mitrakeluarga.com/rfc2350.pdf (versi Bahasa Indonesia)

### 1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP Key milik CISRT MIKA. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

### 1.5. Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

| | |
|---|---|
| Judul | : RFC 2350 CISRT MIKA; |
| Versi | : 1.0 |
| Tanggal Publikasi | : dd month yyyy; |
| Kadaluwarsa | : Dokumen ini valid hingga dokumen terbaru dipublikasikan. |

## 2. Informasi Data/Kontak

### 2.1. Nama Tim

Computer Security Incident Response Team Mitra Keluarga (MIKA)
Disingkat : CSIRT MIKA

### 2.2. Alamat

Mitra Keluarga Kemayoran .....

### 2.3. Zona Waktu

DKI Jakarta (GMT+07:00)

**2.4. Nomor Telepon**

0.....

**2.5. Nomor Fax**

-

**2.6. Telekomunikasi Lain**

(+62) 822 1730 8360 - Whatsapp

**2.7. Alamat Surat Elektronik (E-mail)**

csirt@mitrakeluarga.com

**2.8. Kunci Public (Public Key) dan Informasi/Data Enkripsi lain**

Bits : 4096
ID : 7EA28D7886F00AB9
Key Fingerprint : 1C17 E011 0136 B4EC 17ED 2D42 7EA2 8D78 86F0 0AB9
File PGP key ini tersedia pada :
https://csirt.mitrakeluarga.com/rfc2350/


```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGrIX28BEACjYcnZLkXohoEPPvgoWSeftA9HiX7QdCIZhy3tSPWQ20y/oKyC
+hAzqS5ZYVIu8BYNAPrLrliFyD1K+gfrHCi20cYjXKQ38CTNN5wGOK2sv412aBT2
/tes0FXuzORs0ZrH8VGE4FFoSbA64iY5avco4EgdQLqMQGpFaN+uAnW0jLJFofTr
4t2X7HhKQenr7MDYaiUWJRVE+N8p8Hd5zeU5rKASsVCEAf656mpM1kBT4FcojpXu
GWlhiwMnbHsZlkVhioZL5621JwJVpEfQqyzeSHZbzES7rBq6JjxvyANLgqZtG2T/
zxrABBh7bHZHor8nXE+4zMY9m5ZI+rdkNbxDfijlo2BNWdeFKRm27tFb3axhTrMR
MRu8/A1oo2B+ATtvRzYVh4li23WSzWIQ+iJuXij642ZQ4iA1EGFZdSJ1MmnlRF34
aqr0Aq4RkvECijPhuLcOHr38QTqdoxrmB1uIAug2p2U4pYijX89MBjetD/RCE3XK
rOmdITLvX4viHBpQQDjPPbSDm84M7pN5HSDKHtInitSmP4QQ4Xa6DWF7xNxr2I9s
CkU3GXALb94oVfNU2mPtbVYQvp5zQ5xxfYQhDzZdZ4BsE29aEr1XYnMkISU5Zq5s
d0kt+ubHhSQ7OIWmOnp1x3l3JpK8j1adyMUf34gzSd32oApZdgItknomaQARAQAB
tGhDU0lSVCBNSUtBIChDb21wdXRlciBTZWN1cml0eSBJbmNpZGVudCBSZXNwb25z
ZSBUZWFtIGF0YXUgVFRJUyBNaXRyYSBLZWx1YXJnYSkgPGNzaXJ0QG1pdHJha2Vs
dWFyZ2EuY29tPokCVwQTAQoAQRYhBBwX4BEBNrTsF+0tQn6ijXiG8Aq5BQJqyF9v
AhsDBQkDwmcABQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEH6ijXiG8Aq5
DCUP/iH/Dc9/agUOy3CuPka9WbaQQpRaD77AneF/dNGEaqGz4Pmt7zvcRFpzs7zb
WY/anIckfgOTKKoQhbO6qsgjqY1Zr5EmqrQxYaKXmcCRFRpwFIHJz76I18A41yrK
O3hFXggyAwqaDNPS+bHxYrHsk57aISLMUN6+9nA2UzN3yN2QUTe4AWY9WcHHwlM6
BGtFC7SGGeEiepfy7s+EllFGRCfnGrZYzVP/xb48zAG/UWWTaLevPs0sdhMiyY4g
jjbKnC2QOBm3NGZ+A/3M4pZ0eUAUL2EJSsk8q6pjnqcbhJNuai076Qui7Wuo/4PX
CM6qIYia21Qo+m4zBxQBoZNcMXANiVHAn+7kaCbqsnmzPNzUiUQkfpT8BWSAAFBj
E1odlZTmBEfo6YzAf7otR+XYPVHd/bKAP1ChBqrxiTl0KLWKn33RapREvBSGuU9w
```

```
44PdOHBM7bDz7hc0qAfIB94uU5MsG3Vzvjbf/xGG77tIqg320zq7K9/VwC5wNFxd
i8mNbgna82OtLejfv42EwSdkYVI+zhg97VYAH1K+8qPitrdu6Uwf6o0LVoAYsnTa
QFCd+FalcSMQnPz9AmlN/c2oQ4PYQx5f70HX+GHrqXEjS3fA0tL6RZRUTAm3nxjT
HkpxwCMXpIndKAtImMttZ+eZ2i9K0lpqvyz7W3rU/cTKpVVEuQINBGrIX28BEADJ
Mrvx8SFji2Fr0XoBR7OcBSBethF8fFj9Qi2/L5gkAgY6MFkqEgX/SS4sU87USAUc
rRAXaqEPvwZVRruzBynCOW3JZBXTr28USagcIiSi21pxTY6S7tADQQzh8n48Ydo2
6W5dk/0s5N4mHB/cRp9V4zwdptclGffN3ly3iz/kyqSPylvi07uZ5zKRiC+O4QvY
bjKR2Qb6Pu91CB0C2iERQXVsYrmpzjJ5uu+AgY5zq4DuxTEk0VKtWuTQnvIEkMlP
Z6LHOLIZl2NmAqme7Xs42UQMPqW0JGZOqaCOd+mS8dFINYC3j+s2mVNcHa5vmC0v
llHuUmsmezxwW8KLzzy+2h7OQwCSxrV2QSXgW2+KDjYhxrEaNwBh1KfpWNbct8uI
A0O/HCcNdo/On9oAyp5wiOQqSOgN3OEE+Ghad77RRwqiDJsrXB5zGyBOC8OEoZcS
wHZTEgSSJnUFlM5becWxdQBQLDKHut6PEW9V0O06u5X+M0TF4XzqnUHc8Hl1IGsD
oAiJQor6BCowOdCl/8ymF5coeTcZ18Zges5C7xiTVkIhdixwIAX62t9cXY95QhQM
T0BiubL3m7LI7GBUoy716CLibXZWCvwgjmBVMngyzcUSDkY7R2vwVUrYF7qd+IpT
dQBJGZ0t13NWcz4GnW2ngJxvhQWwQ7U9qUtfAECfrQARAQABiQI8BBgBCgAmFiEE
HBfgEQE2tOwX7S1CfqKNeIbwCrkFAmrIX28CGwwFCQPCZwAACgkQfqKNeIbwCrl9
vw//TU4WcPbWDEYLBhJFFBvBVj+/768jg8E0beGohf8moSoI9A8ng+pxm85Nb47d
IU3wdZeJRptAYRxpDgUMb/VIHZ/RwNyFNUAA9x4mO7D/rfX7ZY3VRSgcnolAaPxi
y5NVp9HqHGyOmi6+BKkK/HUbffcMhnF3YEdfvf7VkIemcD/FsWBHShvOGT4tS4Gg
L/tEQ6GE1O7cGM9Gx1SYViRvTm/5ZLHPIVtwhhBzvmIJiP6j5tZ2JIYWrrZqMeo6
PrmrldIc+X7l2JJM+YjjcBiVbL+cJ86cqmThiW5m1qaRg/SQy4VER+R0HDAHr0oj
068YJ7mlyR+e7WiAtRQmHecTHpKtgZ/GBxcWLhJn+q6FAuRsrrArTHOfFmOgSKt1
a4UeKaEc9Dne0bKK/LYndDM8kRpsrn2Xqk+ZcelxURnrtB5h6FZvdYGzWLf/T9tm
xHyQQDmGNsg6wB/ZTIUygB7dShGmtvB+XBNO0mTEjmD4huVsVWbmiFyfQLfXfS+D
XnyAM9gPiKdCF5Xj6TLjFeWrnm7UuoVQnFgDSGO0D2LDY9xuUBGBuJkm1FuP2TSd
VGPICSY0AQWRMlJKhgaNZ2CFlQvnwNomC1cKv2PRQ7UL/hAD6+7jwI1OD5gHCF2b
Lc8nbLKtB4LvSzLKDhLCydaD3SMzv4LvWFeo7iiuECTjTiI=
=0ikp
-----END PGP PUBLIC KEY BLOCK-----
```

### 2.9. Anggota Tim

Ketua CSIRT MIKA adalah Direktur Teknologi Informasi (IT) Mitra Keluarga. Yang termasuk anggota tim adalah Koordinator Penanggulangan dan Pemulihan Insiden, Unit User Handling, Unit Respon Insiden, Unit Pemulihan Layanan Operasional IT, Unit Tata Kelola dan Kepatuhan dan Narahubung.

### 2.10. Informasi/Data lain

Tidak ada.

### 2.11. Catatan-catatan pada Kontak CSIRT MIKA

Metode yang disarankan untuk menghubungi CISRT MIKA adalah melalui *e-mail* pada alamat csirt@mitrakeluarga.com atau melalui nomor telepon +62....pada hari kerja jam 08:00 - 17:00 WIB.

## 3. Mengenai CSIRT MIKA

### 3.1. Visi

Terwujudnya ketahanan siber pada sistem dan infrastruktur organisasi yang handal.

### 3.2. Misi

Misi dari CSIRT MIKA, yaitu:

a. Membangun koordinasi, kerjasama dan kolaborasi layanan siber di Mitra Keluarga baik dengan pihak internal mupun eksternal;
b. Menyediakan kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi;
c. Mendorong kesadaran keamanan siber pada sumberdaya manusia di lingkungan Mitra Keluarga.

### 3.3. Konstituen

Konstituen CSIRT MIKA yaitu semua penggunakan layanan teknologi informasi di lingkungan Mitra Keluarga.

### 3.4. Sponsorship dan/atau Afiliasi

CSIRT MIKA merupakan bagian dari Departemen IT Mitra Keluarga sehingga pendanaan berasal dari ...

### 3.5. Otoritas

CSIRT MIKA memiliki kewenangan dengan konstituennya dalam penanganan gangguan keamanan siber. CSIRT MIKA dapat berkoordinasi serta bekerja sama dengan pihak lain yang mempunyai kompetensi untuk insiden yang tidak dapat ditangani.

## 4. Kebijakan – Kebijakan

### 4.1. Jenis-jenis Insiden dan Tingkat/Level/Dukungan

CSIRT MIKA melayani penanganan insiden siber dengan jenis berikut :

a. Web Defacement;
b. DDoS;
c. Virus/Malware;
d. Ransomware;
e. Phising;
f. SQL Injection.

Dukungan yang diberikan oleh CISRT MIKA kepada konstituen dapat bervariasi bergantung pada jenis dan dampak insiden.

### 4.2. Kerja sama, Interaksi dan Pengungkapan Infromasi/data

CISRT MIKA akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CISRT MIKA akan dirahasiakan.

### 4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa CSIRT MIKA dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

## 5. Layanan

### 5.1. Layanan Utama

Layanan utama dari CSIRT MIKA yaitu :

#### 5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik yang dikelola oleh masing-masing unit kerja di Mitra Keluarga.

#### 5.1.2. Penanganan Insiden Siber

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan on-site dalam rangka penanggulangan dan penanganan insiden keamanan siber di lingkungan kerja Mitra Keluarga.

### 5.2. Layanan Tambahan

Layanan tambahan dari CSIRT MIKA yaitu :

#### 5.2.1. Penangan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh CSIRT MIKA berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), CSIRT MIKA memberikan informasi statistik terkait layanan ini. Namun layanan ini hanya berlaku apabila syarat- syarat berikut terpenuhi :

a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment*.

#### 5.2.2. Penanganan Artefak Digital

Layanan ini diberikan berupa penanganan artifak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

#### 5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan kepada unit kerja terkait berupa hasil deteksi ancaman terhadap sistem elektronik yang dapat muncul dari perkembangan aplikasi, bisa juga laporan masyarakat berupa hasil deteksi adanya celah keamanan, selanjutnya CSIRT MIKA memberikan informasi statistik terkait layanan ini.

#### 5.2.4. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Dalam layanan ini CSIRT MIKA mendokumentasikan dan mempublikasikan berbagai kegiatan dan informasi yang dilakukan dalam rangkan pembangunan kesadaran dan kepedulian terhadap keamanan siber.

#### 5.2.5. Pendeteksian Serangan

Layanan ini berupa kegiatan analisis untuk mendeteksi adanya serangan terhadap sistem elektronik.

#### 5.2.6. Analisis Risiko Keamanan Siber

Layanan ini berupa kegiatan analisis untuk mendeteksi adanya serangan terhadap sistem elektronik dan dokumentasi kerentanan dan penilaian risiko keamanan informasi yang sesuai dengan standar ISO/IEC 27001.

## 6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@mitrakeluarga.com dengan melampirkan sekurang-kurangnya :

a. Identitas pelapor
b. Bukti insiden berupa foto, screenshoot, video atau log file yang ditemukan.
c. Atau sesuai dengan ketentuan lain yang berlaku.

## 7. Disclaimer

a. Penanganan situs/website yang dikelola bukan oleh Mitra Keluarga tidak ditangani oleh tim CSIRT MIKA, harus oleh tim teknis situs/website terkait.
b. Upaya penanganan insiden dilakukan berdasarkan informasi yang tersedia, kewenangan yang dimiliki, serta sumber daya dan kemampuan teknis yang ada.
c. CSIRT MIKA tidak memberikan jaminan bahwa layanan, panduan, atau rekomendasi yang disampaikan akan menghilangkan seluruh risiko keamanan siber atau mencegah seluruh dampak yang ditimbulkan oleh suatu insiden.